#4

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ４月１２日

出 願 番 号
Application Number: 特願２０００－１１０２６０

出 願 人
Applicant (s): 松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年 １月１９日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２０００－３１１２８７８

【書類名】　特許願

【整理番号】　2022520174

【提出日】　平成12年 4月12日

【あて先】　特許庁長官殿

【国際特許分類】　H04L　9/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　柴田　修

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　湯川　泰平

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　関部　勉

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　齊藤　義行

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　大竹　俊彦

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【書類名】　明細書

【発明の名称】　復号装置および暗復号装置

【特許請求の範囲】

【請求項１】　入力されるデータを復号化する復号装置であって、

前記復号装置は、

装置固有の内部鍵を記憶している内部鍵記憶手段と、

暗号化コンテンツ復号用のコンテンツ鍵を格納するコンテンツ鍵格納手段と、

前記コンテンツ鍵格納手段にコンテンツ鍵が格納されているかの有無を管理する状態遷移管理手段と、

暗号化コンテンツ鍵の復号処理あるいは暗号化コンテンツの復号処理であるかを選択する処理モード選択手段と、

前記状態遷移管理手段の情報と前記処理モード選択手段の情報を基に、暗号化コンテンツ鍵の復号処理が選択されたならば前記内部鍵記憶手段の内部鍵を用いて暗号化コンテンツ鍵を復号化して前記コンテンツ鍵格納手段に格納する、あるいは前記コンテンツ鍵格納手段にコンテンツ鍵が格納されておりかつ暗号化コンテンツの復号処理が選択されたならば前記コンテンツ鍵格納手段に格納されているコンテンツ鍵を用いて暗号化コンテンツを復号化して外部に出力する復号演算処理手段とを具備することを特徴とする復号装置。

【請求項２】　入力されるデータを暗号化あるいは復号化する暗復号装置であって、

前記暗復号装置は、

装置固有の内部鍵を記憶している内部鍵記憶手段と、

暗号化コンテンツ復号用あるいはコンテンツ暗号用のコンテンツ鍵を格納するコンテンツ鍵格納手段と、

コンテンツ鍵の生成処理、暗号化コンテンツ鍵の復号処理、コンテンツの暗号処理あるいは暗号化コンテンツの復号処理かを選択する処理モード選択手段と、

前記処理モード選択手段の情報を基に、コンテンツ暗号用のコンテンツ鍵をランダムに生成し前記コンテンツ鍵格納手段に格納するコンテンツ鍵生成手段と、

前記コンテンツ鍵格納手段にコンテンツ鍵が格納されているかの有無および格

納されているコンテンツ鍵がコンテンツ暗号用あるいは暗号化コンテンツ復号用であるのかを管理する状態遷移管理手段と、

前記状態遷移管理手段の情報と前記処理モード選択手段の情報を基に、コンテンツ鍵の生成処理が選択されたならば前記内部鍵格納手段の内部鍵を用いて前記コンテンツ鍵生成手段で生成されたコンテンツ鍵を暗号化して外部に出力する、あるいは暗号化コンテンツ鍵の復号処理が選択されたならば前記内部鍵記憶手段の内部鍵を用いて暗号化コンテンツ鍵を復号化して、得られたコンテンツ復号用のコンテンツ鍵を前記コンテンツ鍵格納手段に格納する、あるいは前記コンテンツ鍵格納手段にコンテンツ暗号用のコンテンツ鍵が格納されておりかつコンテンツの暗号処理が選択されたならば前記コンテンツ鍵格納手段に格納されているコンテンツ鍵を用いてコンテンツを暗号化して外部に出力する、あるいは前記コンテンツ鍵格納手段に暗号化コンテンツ復号用のコンテンツ鍵が格納されておりかつ暗号化コンテンツの復号処理が選択されたならば前記コンテンツ鍵格納手段に格納されているコンテンツ鍵を用いて暗号化コンテンツを復号化して外部に出力する暗復号演算処理手段とを具備することを特徴とする暗復号装置。

【請求項３】　前記復号装置において、検証パターンを記憶しコンテンツ鍵の正否を判断するコンテンツ鍵検証手段をさらに具備し、

前記処理モード選択手段は暗号化検証パターンの復号処理であるかの選択も行ない、

前記状態遷移管理手段は検証パターンの正否の管理も行ない、

暗号化コンテンツ鍵の復号化を行なった後に、

前記状態遷移管理手段の情報と前記処理モード選択手段の情報を基に、暗号化検証パターンの復号処理が選択されたならば前記コンテンツ鍵格納手段に格納されているコンテンツ鍵を用いて暗号化検証パターンを前記復号演算手段あるいは前記暗復号演算手段で復号演算し、復号化された検証パターンを前記コンテンツ鍵検証手段に出力し、前記コンテンツ鍵検証手段で記憶している検証パターンと比較して一致しているかどうかの正否を外部に出力し、一致したときのみ暗号化コンテンツの復号処理を行なうことを特徴とする請求項１記載の復号装置。

【請求項４】　暗号復号装置において、検証パターンを記憶しコンテンツ鍵の

正否を判断するコンテンツ鍵検証手段をさらに具備し、

前記処理モード選択手段は暗号化検証パターンの復号処理であるかの選択も行ない、

前記状態遷移管理手段は検証パターンの正否の管理も行ない、

暗号化コンテンツ鍵の復号化を行なった後に、

前記状態遷移管理手段の情報と前記処理モード選択手段の情報を基に、暗号化検証パターンの復号処理が選択されたならば前記コンテンツ鍵格納手段に格納されているコンテンツ鍵を用いて暗号化検証パターンを前記復号演算手段あるいは前記暗復号演算手段で復号演算し、復号化された検証パターンを前記コンテンツ鍵検証手段に出力し、前記コンテンツ鍵検証手段で記憶している検証パターンと比較して一致しているかどうかの正否を外部に出力し、一致したときのみ暗号化コンテンツの復号処理を行なうことを特徴とする請求項２記載の暗復号装置。

【請求項５】　前記復号装置において、暗号化コンテンツ鍵を記憶している外部装置との間で相互認証を行なう相互認証手段をさらに具備し、

前記状態遷移管理手段は相互認証の成否の管理も行ない、

前記コンテンツ鍵の生成処理あるいは前記暗号化コンテンツ鍵の復号処理を行なう前に、前記相互認証手段を用いて外部装置との間で相互認証を行ない、

相互認証が成立したときのみ暗号化コンテンツの復号化あるいはコンテンツの暗号化を行なうことを特徴とする請求項１あるいは３記載の復号装置。

【請求項６】　前記暗復号装置において、暗号化コンテンツ鍵を記憶している外部装置との間で相互認証を行なう相互認証手段をさらに具備し、

前記状態遷移管理手段は相互認証の成否の管理も行ない、

前記コンテンツ鍵の生成処理あるいは前記暗号化コンテンツ鍵の復号処理を行なう前に、前記相互認証手段を用いて外部装置との間で相互認証を行ない、

相互認証が成立したときのみ暗号化コンテンツの復号化あるいはコンテンツの暗号化を行なうことを特徴とする請求項２あるいは４記載の暗復号装置。

【請求項７】　前記内部鍵記憶手段に記憶している内部鍵が複数個あり、外部から入力される情報を基に、その中からひとつを選択して使用することを特徴とする請求項１あるいは３あるいは５記載の復号装置。

【請求項８】　前記内部鍵記憶手段に記憶している内部鍵が複数個あり、外部から入力される情報を基に、その中からひとつを選択して使用することを特徴とする請求項２あるいは４あるいは６記載の暗復号装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、音楽、画像、映像、ゲームなどのディジタルコンテンツを暗号化あるいは復号化を行なう装置において、暗号化あるいは復号化を行なうのに用いるコンテンツ鍵の機密性を高め、かつコンテンツの暗号化あるいは復号化を不正に動作させるのを防止する技術に関する。

【０００２】

【従来の技術】

音楽、画像、映像、ゲームなどのディジタルコンテンツの著作権者の権利や流通業者の利益を保護するために、通信の傍受、盗聴、なりすましなどによる不正入手や、受信したデータを記憶した記録媒体における違法複製、違法改ざんなどの不正行為を防止することが課題となり、正規システムの判別、データスクランブルを行なう暗号/認証などの著作物保護技術が必要となっている。

【０００３】

近年、各種民生機器にも著作権保護技術が搭載され始めており、一般的に、コンテンツの再生録音機器における回路構成は、暗号／復号演算を行なう暗復号装置と、その暗復号装置を制御するマスター制御装置を用いて暗号／復号処理を実現している。

【０００４】

暗号化されたコンテンツ（暗号化コンテンツ）と、そのコンテンツの復号処理に用いる暗号化されている鍵（暗号化コンテンツ鍵）を用いる再生処理は、具体的に次のように行っている。まず、再生録音機器内のマスター制御装置が暗号化コンテンツと、暗号化コンテンツ鍵を記憶しているメモリ装置からデータを読み込む。マスター制御装置が、暗号化コンテンツ鍵を暗復号装置に入力し、暗復号装置内でコンテンツ鍵を得る。その後、マスター制御装置が、暗号化コンテンツ

を暗復号装置に入力することにより、マスター制御装置が保持しているコンテンツ鍵で暗号化コンテンツの復号を行い、マスター制御装置に出力する。以上が暗号コンテンツの再生処理の流れである。

【０００５】

また、録音処理は次のように行われる。マスター制御装置が暗復号装置にコンテンツ鍵生成命令を発行することにより、暗号回路内部にコンテンツの暗号化するのに用いるコンテンツ鍵が生成されると共に、そのコンテンツ鍵を暗号化した暗号コンテンツ鍵が、マスター制御装置に出力される。次に、マスター制御装置が、暗復号装置にコンテンツを入力することにより、暗復号装置がコンテンツの暗号化を行い、マスター制御装置に暗号化コンテンツを出力する。その後、マスター制御装置がメモリ装置に対し、暗号化コンテンツとその暗号化コンテンツ鍵を転送することで、録音処理が終了する。

【０００６】

【発明が解決しようとする課題】

ここで課題となるのは、マスター制御装置に耐タンパ性がない場合に、不正に暗復号装置を動作させることができ、例えば、暗復号装置にコンテンツ鍵を設定すること無く暗復装置内の初期の鍵を用いてコンテンツの暗号化あるいは復号化を行うことができため、暗復号装置の初期鍵が何らかの要因で漏洩したときに、暗号／復号のアルゴリズムを解析することが容易となり問題となる。

【０００７】

本発明の目的は、コンテンツを暗号化あるいは復号化を行なう装置において、コンテンツ鍵を正常に設定することなくコンテンツの暗号化あるいは復号化を不正に動作させるのを防止する装置を提供する。

【０００８】

【課題を解決するための手段】

本発明に係る復号装置は、入力されるデータを復号化する復号装置であって、前記復号装置は、装置固有の内部鍵を記憶している内部鍵記憶手段と、暗号化コンテンツ復号用のコンテンツ鍵を格納するコンテンツ鍵格納手段と、前記コンテンツ鍵格納手段にコンテンツ鍵が格納されているかの有無を管理する状態遷移管

理手段と、暗号化コンテンツ鍵の復号処理あるいは暗号化コンテンツの復号処理かを選択する処理モード選択手段と、前記状態遷移管理手段の情報と前記処理モード選択手段の情報を基に、暗号化コンテンツ鍵の復号処理が選択されたならば前記内部鍵記憶手段の内部鍵を用いて暗号化コンテンツ鍵を復号化して前記コンテンツ鍵格納手段に格納する、あるいは前記コンテンツ鍵格納手段にコンテンツ鍵が格納されておりかつ暗号化コンテンツの復号処理が選択されたならば前記コンテンツ鍵格納手段に格納されているコンテンツ鍵を用いて暗号化コンテンツを復号化して外部に出力する復号演算処理手段とを具備し、そのことにより上記目的が達成される。

【０００９】

本発明に係る暗復号装置は、入力されるデータを暗号化あるいは復号化する暗復号装置であって、前記暗復号装置は、装置固有の内部鍵を記憶している内部鍵記憶手段と、暗号化コンテンツ復号用あるいはコンテンツ暗号用のコンテンツ鍵を格納するコンテンツ鍵格納手段と、コンテンツ鍵の生成処理、暗号化コンテンツ鍵の復号処理、コンテンツの暗号処理あるいは暗号化コンテンツの復号処理かを選択する処理モード選択手段と、前記処理モード選択手段の情報を基に、コンテンツ暗号用のコンテンツ鍵をランダムに生成し前記コンテンツ鍵格納手段に格納するコンテンツ鍵生成手段と、前記コンテンツ鍵格納手段にコンテンツ鍵が格納されているかの有無および格納されているコンテンツ鍵がコンテンツ暗号用あるいは暗号化コンテンツ復号用であるのかを管理する状態遷移管理手段と、前記状態遷移管理手段の情報と前記処理モード選択手段の情報を基に、コンテンツ鍵の生成処理が選択されたならば前記内部鍵格納手段の内部鍵を用いて前記コンテンツ鍵生成手段で生成されたコンテンツ鍵を暗号化して外部に出力する、あるいは暗号化コンテンツ鍵の復号処理が選択されたならば前記内部鍵記憶手段の内部鍵を用いて暗号化コンテンツ鍵を復号化して、得られたコンテンツ復号用のコンテンツ鍵を前記コンテンツ鍵格納手段に格納する、あるいは前記コンテンツ鍵格納手段にコンテンツ暗号用のコンテンツ鍵が格納されておりかつコンテンツの暗号処理が選択されたならば前記コンテンツ鍵格納手段に格納されているコンテンツ鍵を用いてコンテンツを暗号化して外部に出力する、あるいは前記コンテンツ

鍵格納手段に暗号化コンテンツ復号用のコンテンツ鍵が格納されておりかつ暗号化コンテンツの復号処理が選択されたならば前記コンテンツ鍵格納手段に格納されているコンテンツ鍵を用いて暗号化コンテンツを復号化して外部に出力する暗復号演算処理手段とを具備し、そのことにより上記目的が達成される。

【００１０】

前記復号装置あるいは暗号復号装置において、検証パターンを記憶しコンテンツ鍵の正否を判断するコンテンツ鍵検証手段をさらに具備し、前記処理モード選択手段は暗号化検証パターンの復号処理かの選択も行ない、前記状態遷移管理手段は検証パターンの正否の管理も行ない、暗号化コンテンツ鍵の復号化を行なった後に、前記状態遷移管理手段の情報と前記処理モード選択手段の情報を基に、暗号化検証パターンの復号処理が選択されたならば前記コンテンツ鍵格納手段に格納されているコンテンツ鍵を用いて暗号化検証パターンを前記復号演算手段あるいは前記暗復号演算手段で復号演算し、復号化された検証パターンを前記コンテンツ鍵検証手段に出力し、前記コンテンツ鍵検証手段で記憶している検証パターンと比較して一致しているかどうかの正否を外部に出力し、一致したときのみ暗号化コンテンツの復号処理を行なうようにしてもよい。

【００１１】

前記復号装置あるいは暗復号装置において、暗号化コンテンツ鍵を記憶している外部装置との間で相互認証を行なう相互認証手段をさらに具備し、前記状態遷移管理手段は相互認証の成否の管理も行ない、前記コンテンツ鍵の生成処理あるいは前記暗号化コンテンツ鍵の復号処理を行なう前に、前記相互認証手段を用いて外部装置との間で相互認証を行ない、相互認証が成立したときのみ暗号化コンテンツの復号化あるいはコンテンツの暗号化を行なうようにしてもよい。

【００１２】

前記内部鍵記憶手段に記憶している内部鍵が複数個あり、外部から入力される情報を基に、その中からひとつを選択して使用するようにしてもよい。

【００１３】

【発明の実施の形態】

以下に本発明の原理と実施の形態を添付の図面を用いて説明する。

【００１４】

（実施の形態１）

図１は、本発明の実施の形態１における構成図を示し、ホストであるマスター装置１００から入力される情報を基にデータを復号化する復号装置１０１を示す。

【００１５】

復号装置１０１は、装置固有の内部鍵を一つあるいは複数記憶し、マスター装置１００から入力される内部鍵選択情報１０６を基に格納されている鍵の中から一つの内部鍵を選択する内部鍵記憶手段１０５と、暗号化コンテンツ復号用のコンテンツ鍵を格納するコンテンツ鍵格納手段１０７と、コンテンツ鍵格納手段１０７にコンテンツ鍵が格納されているかの有無を管理する状態遷移管理手段１１１と、マスター装置１００から入力される処理モード情報１０８を基に暗号化コンテンツ鍵の復号処理あるいは暗号化コンテンツの復号処理かを選択する処理モード選択手段１０９と、状態遷移管理手段１１１の情報と処理モード選択手段１０９の情報を基に、暗号化コンテンツ鍵の復号処理が選択されたならば内部鍵記憶手段１０５で選択された内部鍵を用いてマスター装置１００から入力データ１０２として入力される暗号化コンテンツ鍵を復号化してコンテンツ鍵格納手段１０７に格納する、あるいはコンテンツ鍵格納手段１０７にコンテンツ鍵が格納されておりかつ暗号化コンテンツの復号処理が選択されたならばコンテンツ鍵格納手段１０７に格納されているコンテンツ鍵を用いてマスター装置１００から入力データ１０２として入力される暗号化コンテンツを復号化して出力データ１０４としてマスター装置１００に出力する復号演算処理手段１０３とを備える。

【００１６】

なお、内部鍵記憶手段１０５は外部からアクセスすることはできない領域であり、装置固有の内部鍵をハードワイヤ、ＲＯＭあるいは不揮発メモリとして実装される。

【００１７】

また、復号演算手段１０３で行なわれる復号方法は暗号／復号のアルゴリズムであえば何を用いてもよく、例えばＤＥＳ(Data Encryption Standard)などを用

いればよい。

【００１８】

また、内部鍵、コンテンツ鍵の鍵長は何ビットでもよく、例えば５６ビットとすればよい。

【００１９】

以上のように、本実施の形態の復号装置は、コンテンツ鍵を復号装置内部にある装置固有かつ秘密な内部鍵で暗号化した状態で入力し、復号装置内で解読して使用するため、コンテンツ復号用のコンテンツ鍵の機密性を高めることができ、かつ暗号化コンテンツの復号化を暗号化コンテンツ復号用のコンテンツ鍵がコンテンツ鍵格納手段に正しく格納されている場合にのみ行なう構成としたので、コンテンツの復号化を不正に動作させることを防止できるという効果がある。

【００２０】

（実施の形態２）

図２は、本発明の実施の形態２における暗復号装置２０１を示す。

【００２１】

暗復号装置２０１は、装置固有の内部鍵を一つあるいは複数記憶し、マスター装置２００から入力される内部鍵選択情報１０６を基に格納されている鍵の中から一つの内部鍵を選択する内部鍵記憶手段１０５と、暗号化コンテンツ復号用あるいはコンテンツ暗号用のコンテンツ鍵を格納するコンテンツ鍵格納手段１０７と、マスター装置２００から入力される処理モード情報１０８を基にコンテンツ鍵の生成処理、暗号化コンテンツ鍵の復号処理、コンテンツの暗号処理あるいは暗号化コンテンツの復号処理かを選択する処理モード選択手段１０９と、前記処理モード選択手段の情報を基に、コンテンツ暗号用のコンテンツ鍵をランダムに生成し前記コンテンツ鍵格納手段に格納するコンテンツ鍵生成手段２１３と、コンテンツ鍵格納手段１０７にコンテンツ鍵が格納されているかの有無および格納されているコンテンツ鍵がコンテンツ暗号用あるいは暗号化コンテンツ復号用であるのかを管理する状態遷移管理手段１１１と、状態遷移管理手段１１１の情報と処理モード選択手段１０９の情報を基に、コンテンツ鍵の生成処理が選択されたならば内部鍵記憶手段１０５で選択された内部鍵を用いてコンテンツ鍵生成手

段２１３で生成されたコンテンツ鍵を暗号化して出力データ１０４としてマスター装置２００に出力する、あるいは暗号化コンテンツ鍵の復号処理が選択されたならば内部鍵格納手段１０５の内部鍵を用いてマスター装置２００から入力データ１０２として入力される暗号化コンテンツ鍵を復号化して、得られたコンテンツ復号用のコンテンツ鍵をコンテンツ鍵格納手段１０７に格納する、あるいはコンテンツ鍵格納手段１０７にコンテンツ暗号用のコンテンツ鍵が格納されておりかつコンテンツの暗号処理が選択されたならばコンテンツ鍵格納手段１０７に格納されているコンテンツ鍵を用いてマスター装置２００から入力データ１０２として入力されるコンテンツを暗号化して出力データ１０４としてマスター装置２００に出力する、あるいはコンテンツ鍵格納手段１０７に暗号化コンテンツ復号用のコンテンツ鍵が格納されておりかつ暗号化コンテンツの復号処理が選択されたならばコンテンツ鍵格納手段１０７に格納されているコンテンツ鍵を用いてマスター装置２００から入力データ１０２として入力される暗号化コンテンツを復号化して出力データ１０４としてマスター装置２００に出力する暗復号演算処理手段２０３とを備える。

【００２２】

なお、内部鍵記憶手段１０５は外部からアクセスすることはできない領域であり、装置固有の内部鍵をハードワイヤ、ＲＯＭあるいは不揮発メモリとして実装される。

【００２３】

また、暗復号演算手段１０３で行なわれる暗号および復号の方法は暗号／復号アルゴリズムであえば何を用いてもよく、例えばＤＥＳ(Data Encryption Standard)などを用いればよい。

【００２４】

また、内部鍵、コンテンツ鍵の鍵長は何ビットでもよく、例えば５６ビットとすればよい。

【００２５】

また、コンテンツ鍵の生成方法はランダムな整数を発生する方法なら何を用いてよく、例えば常時動作するクロックカウンタなどを用いればよい。

【００２６】

以上のように、本実施の形態の暗復号装置は、コンテンツ暗号用のコンテンツ鍵をランダムに生成し、マスター装置には生成したコンテンツ鍵を内部鍵で暗号化して出力するのでコンテンツ暗号用のコンテンツ鍵の機密性を高めることができ、かつコンテンツの暗号化はコンテンツ暗号用のコンテンツ鍵がコンテンツ鍵格納手段に正しく格納されている場合のみ行なう、また暗号化コンテンツの復号化は暗号化コンテンツ復号用のコンテンツ鍵がコンテンツ鍵格納手段に正しく格納されている場合のみ行なう構成としたので、コンテンツの復号化あるいは暗号化を不正に動作させることを防止できるという効果がある。

【００２７】

（実施の形態３）

図３は、本発明の実施の形態３における構成図を示し、図１で示した復号装置３０１において、検証パターンを記憶しコンテンツ鍵の正否を判断するコンテンツ鍵検証手段３１５をさらに備えるようにした。処理モード選択手段１０９は暗号化検証パターンの復号処理かの選択も行ない、状態遷移管理手段１１１は検証パターンの正否の管理も行ない、暗号化コンテンツ鍵の復号化を行なった後に、状態遷移管理手段１１１の情報と処理モード選択手段１０９の情報を基に、暗号化検証パターンの復号処理が選択されたならばコンテンツ鍵格納手段１０７に格納されているコンテンツ鍵を用いて暗号化検証パターンを復号演算手段１０３で復号演算して復号化された検証パターンをコンテンツ鍵検証手段３１５に出力し、コンテンツ鍵検証手段３１５で記憶している検証パターンと比較して一致しているかどうかの正否を外部に出力し、一致したときのみ暗号化コンテンツの復号処理を行なうようにする。

【００２８】

以上のように、本実施の形態の復号装置は、検証パターンを用いてコンテンツ鍵格納手段に格納されているコンテンツ鍵の正当性を検証し、正しい鍵と判断されたときのみ暗号化コンテンツの復号化を行なうようにしたので、より強固にコンテンツの復号化を不正に動作させることを防止できるという効果がある。

【００２９】

なお、本実施の形態３の内容を図２に示す暗復号装置に適用しても、同様の効果を得ることが可能であることは自明である。

【００３０】

（実施の形態４）

図４は、本発明の実施の形態４における構成図を示し、図１で示した復号装置において、暗号化コンテンツ鍵を記憶しているメモリ装置４１６との間で相互認証を行なう相互認証手段４１７をさらに備えるようにした。状態遷移管理手段１１１は相互認証の成否の管理も行ない、暗号化コンテンツ鍵の復号処理を行なう前に、相互認証手段４１７を用いてメモリ装置の相互認証手段４１４との間で相互認証を行ない、相互認証が成立したときのみ暗号化コンテンツの復号化を行なうようにする。

【００３１】

以上のように、本実施の形態の復号装置は、暗号化コンテンツ鍵を記憶している装置と相互認証を行ない、相互認証が成立したときのみコンテンツの復号化を行なうようして暗号化コンテンツ鍵の読み先の正当性まで確認するようにしたので、より一層強固にコンテンツの復号化を不正に動作させることを防止できるという効果がある。

【００３２】

なお、本実施の形態４の内容を図２に示す暗復号装置に適用しても、同様の効果を得ることが可能であることは自明である。

【００３３】

【発明の効果】

以上のことより本発明は以下のような効果を奏する。本発明に係る復号装置は、コンテンツ鍵を復号装置内部にある装置固有かつ秘密な内部鍵で暗号化した状態で入力し、復号装置内で解読して使用するため、コンテンツ復号用のコンテンツ鍵の機密性を高めることができ、かつ暗号化コンテンツの復号化を暗号化コンテンツ復号用のコンテンツ鍵がコンテンツ鍵格納手段に正しく格納されている場合にのみ行なう構成としたので、コンテンツの復号化を不正に動作させることを防止できるという効果がある。

【００３４】

また、本発明に係る暗復号装置は、コンテンツ暗号用のコンテンツ鍵をランダムに生成し、マスター装置には生成したコンテンツ鍵を内部鍵で暗号化して出力するのでコンテンツ暗号用のコンテンツ鍵の機密性を高めることができ、かつコンテンツの暗号化はコンテンツ暗号用のコンテンツ鍵がコンテンツ鍵格納手段に正しく格納されている場合のみ行なう、また暗号化コンテンツの復号化は暗号化コンテンツ復号用のコンテンツ鍵がコンテンツ鍵格納手段に正しく格納されている場合のみ行なう構成としたので、コンテンツの復号化あるいは暗号化を不正に動作させることを防止できるという効果がある。

【００３５】

また、本発明に係る復号装置は、検証パターンを用いてコンテンツ鍵格納手段に格納されているコンテンツ鍵の正当性を検証し、正しい鍵と判断されたときのみ暗号化コンテンツの復号化を行なうようにしたので、より強固にコンテンツの復号化を不正に動作させることを防止できるという効果があり、暗復号装置に適用しても、同様の効果を得ることが可能である。

【００３６】

また、本発明に係る復号装置は、暗号化コンテンツ鍵を記憶している装置と相互認証を行ない、相互認証が成立したときのみコンテンツの復号化を行なうようにして暗号化コンテンツ鍵の読み先の正当性まで確認するようにしたので、より一層強固にコンテンツの復号化を不正に動作させることを防止できるという効果があり、暗復号装置に適用しても、同様の効果を得ることが可能である。

【図面の簡単な説明】

【図１】

実施の形態１の構成を示す構成図

【図２】

実施の形態２の構成を示す構成図

【図３】

実施の形態３の構成を示す構成図

【図４】

実施の形態４の構成を示す構成図

【符号の説明】

１００，２００，３００，４００　マスター装置

１０１，３０１，４０１　復号装置

２０１　暗復号装置

１０２　入力データ

１０３　復号演算処理手段

２０３　暗復号演算処理手段

１０４　出力データ

１０５　内部鍵記憶手段

１０６　内部鍵選択情報

１０７　コンテンツ鍵格納手段

１０８　処理モード情報

１０９　処理モード選択手段

１１１　状態遷移管理手段

２１３　コンテンツ鍵生成手段

３１０　正否情報

３１５　コンテンツ鍵検証手段

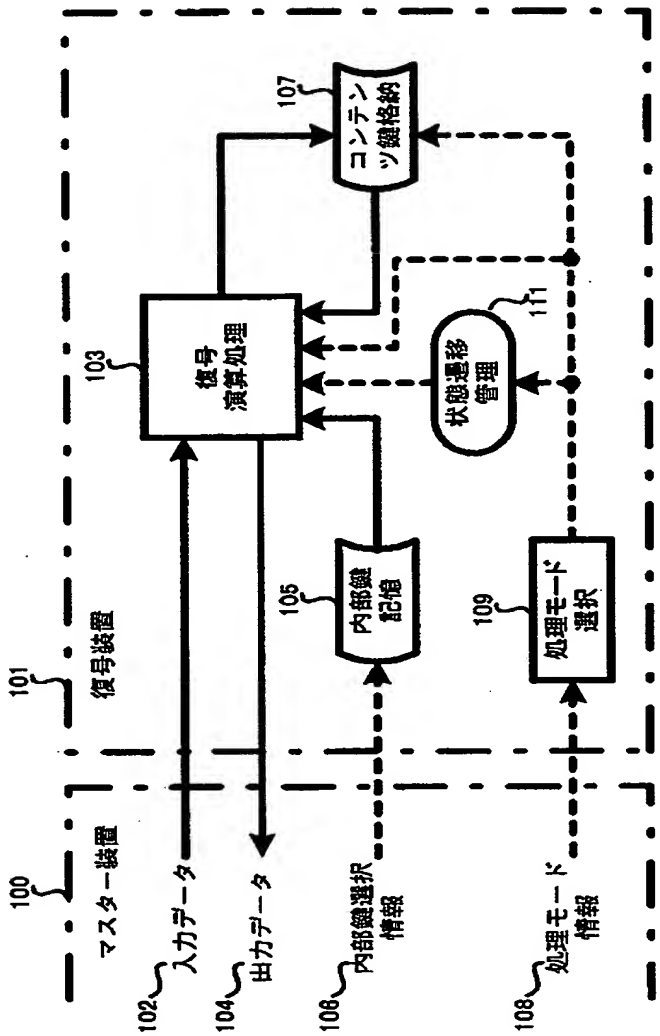
４１２　暗号化コンテンツ鍵格納手段

４１４，４１７　相互認証手段

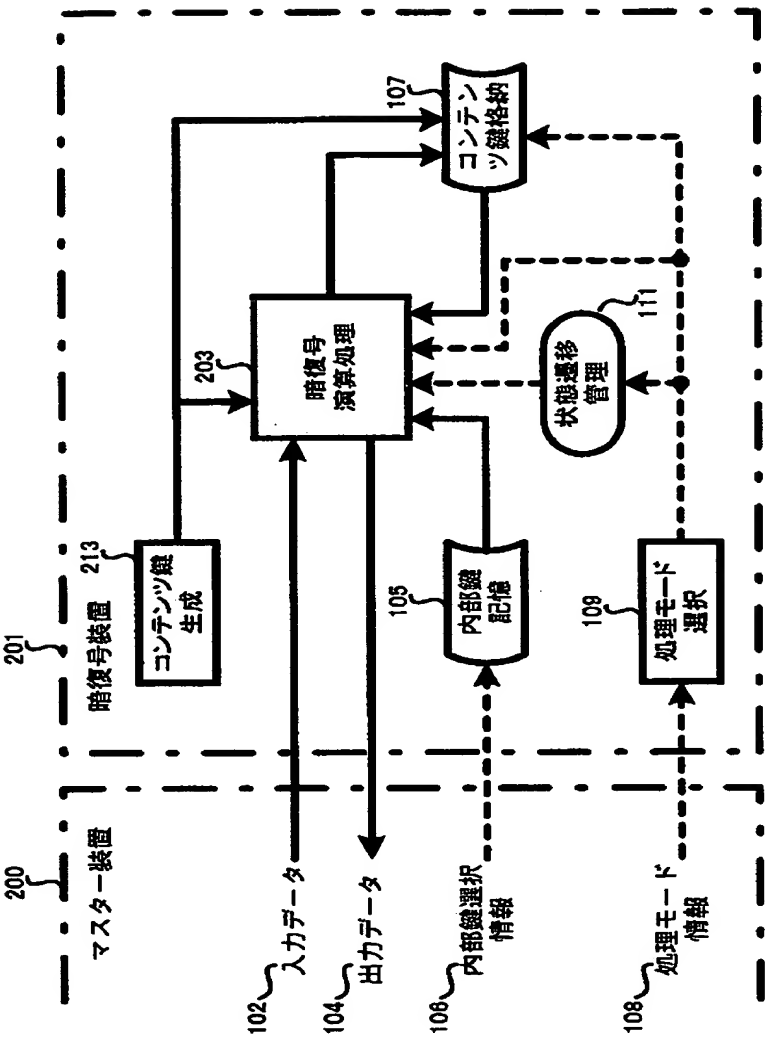
４１６　メモリ装置

【書類名】　　図面

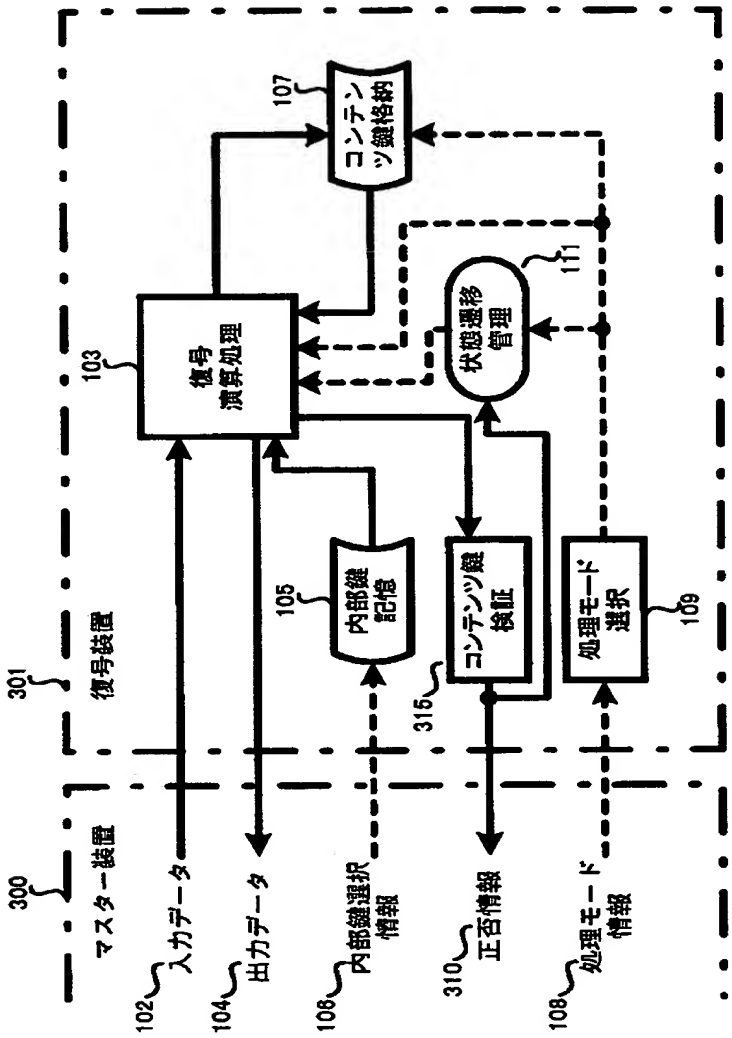
【図１】


100
マスター装置
101
復号装置
102
入力データ
103
復号演算処理
104
出力データ
105
内部鍵記憶
106
内部鍵選択情報
107
コンテンツ鍵格納
108
処理モード情報
109
処理モード選択
111
状態遷移管理

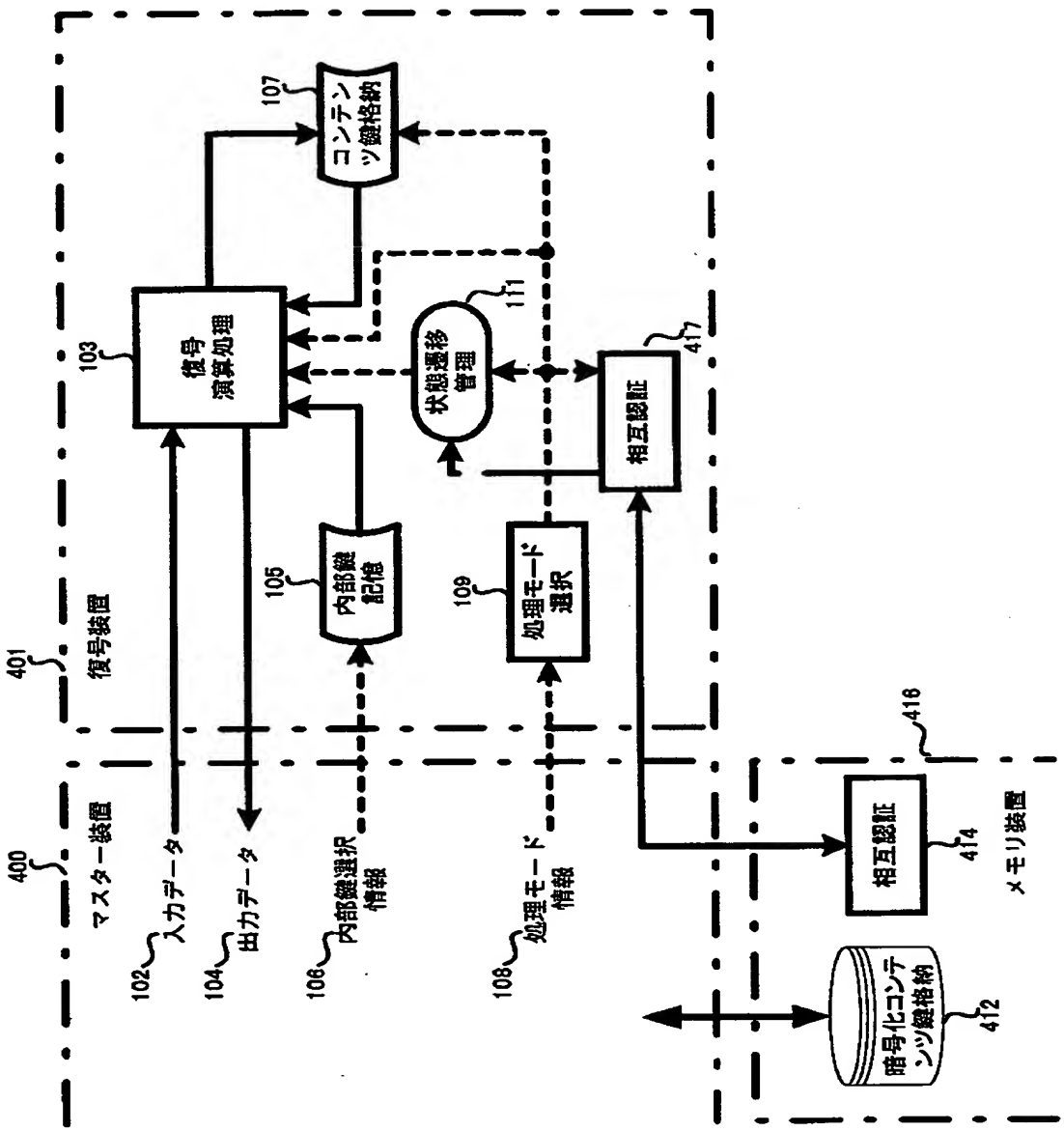
【図２】


200
マスター装置
201
暗復号装置
213
コンテンツ鍵生成
203
暗復号演算処理
107
コンテンツ鍵格納
105
内部鍵記憶
111
状態遷移管理
109
処理モード選択
102
入力データ
104
出力データ
106
内部鍵選択情報
108
処理モード情報

【図３】


300
マスター装置
301
復号装置
102
入力データ
104
出力データ
103
復号演算処理
107
コンテンツ鍵格納
105
内部鍵記憶
106
内部鍵選択情報
111
状態遷移管理
315
コンテンツ鍵検証
310
正否情報
109
処理モード選択
108
処理モード情報

【図４】


400
マスター装置
401
復号装置
402
メモリ装置
102
入力データ
103
復号演算処理
104
出力データ
105
内部鍵記憶
106
内部鍵選択情報
107
コンテンツ鍵格納
108
処理モード情報
109
処理モード選択
111
状態遷移管理
412
暗号化コンテンツ鍵格納
414
相互認証
416
417
相互認証

【書類名】　要約書

【要約】

【課題】　コンテンツを暗号化あるいは復号化を行なう装置において、コンテンツ鍵を正常に設定することなくコンテンツの暗号化あるいは復号化を不正に動作させるのを防止する装置を提供する。

【解決手段】　コンテンツを暗号化あるいは復号化を行なう暗復号装置において、コンテンツ鍵の設定処理を管理し、コンテンツの暗号化あるいは復号化をコンテンツ鍵が暗復号装置に正しく設定されている場合にのみ動作させる構成とした。

【選択図】　図１

出 願 人 履 歴 情 報

識別番号　〔０００００５８２１〕

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社

(Translation)

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application : April 12, 2000

Application Number : Patent Appln. No. 2000-110260

Applicant(s) : MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.

Wafer of the Patent Office

January 19, 2001

Kozo OIKAWA

Commissioner,
Patent Office

Seal of Commissioner of the Patent Office

Appln. Cert. No. Appln. Cert. Pat. 2000-3112878